An analytics-driven approach to the "de-risking" dilemma

By using emerging technologies, organizations can transform the way they manage risks to add value to the business while adhering to compliance commitments, write **Ivan Zasarsky** and **Chad Olsen**

Financial institutions are finding that taking the measures required to increase control over the movement of money to combat money laundering and terrorist financing doesn't just ramp up costs, it can also have negative consequences.

Tighter regulations covering money laundering and terrorist financing have led to massive increases in staff numbers and more complex internal control frameworks for banks and other financial institutions.

Not surprisingly, these institutions are concerned about the deepening risks associated with financial crime. As a result, the Asia-Pacific region's financial crime compliance industry has grown significantly in the past five years.

A 2016 LexisNexis study estimated that annual anti-money laundering compliance budgets in Asia now amount to US$1.5 billion. Recently, some global network banks have indicated employment of over 7,000 compliance team members to manage the tighter vetting process.

The impact on Hong Kong has been stark. Nearly 60,000 suspicious transactions were reported to the Joint Financial Intelligence Unit here in the first nine months of 2016. At the same time, the Hong Kong Monetary Authority seized assets worth HK$105 million after enhancing its reporting and monitoring requirements. Hong Kong can impose fines of up to HK$10 million for each breach.

On the horns of a dilemma

Despite some success, the tightening of international regulatory standards is having unintended consequences. Financial institutions are adopting a "just say no" approach instead of targeting the risks that matter. This "broadsword" response to de-risking has led to the termination of entire portfolios and relationships with individual customers or businesses deemed as high risk – a dramatic change in the application of "know your customer" standards.

As a result, financial institutions face a dilemma. In their quest to comply with the regulations covering money laundering and terrorist financing, they are at risk of being accused of denying basic services to customers that do not present a risk. This affects genuine individuals and businesses, resulting in a diminished customer experience and a loss of legitimate business and revenue.

A recent survey by the HKMA suggests that it is now much harder for businesses and individuals to access basic banking services in the city. To open a business bank account, for instance, applicants must have supporting documents specifying the source of funds, the nature of the company's business and its likely money transactions.

For financial institutions, the necessity to comply with regulations while delivering a positive customer experience can be hard to manage. After all, not every customer is a risk, and taking a blanket approach does not allow them to focus their efforts on the financial crime risks that matter.

Identify the risks that matter

But what if there was an alternative to managing this de-risking dilemma – one that allowed organizations, in effect, to move away from using a blunt-edged broadsword to using a sharpened scalpel?

In our experience working with leading financial institutions, we're finding that successful organizations are adopting a risk-based and analytics-driven approach to more accurately define the risks at each stage of customer engagement and reconcile the gaps.

A risk-based approach doesn't only isolate the risks that matter, it also reduces operational inefficiencies. Ultimately, it can lead to legitimate clients being able to bank without unnecessary and intrusive scrutiny. Institutions that adopt this approach can also target the risks that matter by focusing on an in-depth "know your customer" effort.

Risky business requires a risk-sensitive scale

Several international banks have now incorporated a risk-based approach

in their account-opening processes. However, many other areas of the customer life cycle still need to play catch-up – including transaction monitoring, fraud monitoring, sanction screening and case management.

Take sanction payment screening, for example. Here, a broadsword approach may mean all transactions with queries go through the same complex investigative process, regardless of the actual risks of the transaction. This can delay transaction processing and add unnecessary costs.

Transaction monitoring – where rules are based only on transactions – is another prime example of an area that can benefit from a risk-based approach supported by advanced analytics. Here, adopting such a strategy means the scope and complexity of the monitoring process is determined on a risk-sensitive basis. The institution sets the levels of monitoring within its different business units, depending on the respective risk factors in those units.

A risk-based approach can also extend to knowing and understanding customers, and updating their risk profiles on a risk-sensitive basis. This identifies any discrepancies between a given transaction and a customer's risk profile, and can also allow for differentiated monitoring based on a customer's level of money laundering or terrorist financing risk.

In this way, organizations can monitor the overall relationship with a customer, over and above individual accounts.

The result? Better monitoring of customer accounts with the greatest financial crime risks. In the longer term, that means organizations file fewer, but more accurate, reports with financial intelligence units. As such reports play a major role in determining ongoing customer account due diligence, this also substantially benefits legitimate customer accounts in the long term. More targeted, ongoing customer account due diligence can spare customers from additional questions or requests for documents.

Don't stop there, get intelligent

At the same time, embedding automated processes into business models can improve efficiency. Data analytics tools can be used for customer due diligence, for example, or to identify and track all attempts at fraudulent activity in an organization and map them to high-risk profiles at the early stages of customer engagement.

Technology can be used at every touchpoint over a customer life cycle. Improved methods may leverage robotics and the emerging use of blockchain. Data visualization and tangible dashboards with comprehensive reports can drive decisions and boost business outcomes.

Businesses can get better insights by using the power of data analytics to identify inefficiencies in financial crime processes and quickly address risk vulnerabilities.

Automating the monitoring processes can also reduce the time and staff numbers needed to conduct investigations, and achieve greater accuracy in identifying potential risks.

Then there's building customer risk profiles. Using technology to detect patterns and anomalies here can cut costs by reducing work hours, as well as protecting legitimate businesses and allowing for informed decision making when it comes to targeting the areas of highest risk.

The resulting risk visibility can also allow businesses to identify new opportunities, highlighting the areas in which a business can improve sales and gain profits.

Transform your risk burden into opportunities

Organizations can transform increasing compliance burdens into a competitive advantage if they have the right methods and frameworks in place.

By using emerging technologies – including analytics, robotics and automation – they can transform the way they manage risks to do business safely and drive revenue. By searching for synergies between financial crime intelligence and customer intelligence initiatives, they can identify opportunities to improve customer service and add value to the business. Simply put, they can satisfy regulatory and compliance commitments without compromising the customer experience.

Organizations that future-proof their risk strategies in this way are finding that they can inject a new way of thinking beyond merely de-risking.

Ivan Zasarsky is Forensic Partner and **Chad Olsen** is Forensic Director at Deloitte China